Network penetration testing (ethical hacking)

A Graduate Project Submitted to the Department of Information Security of the College of Information Technology, University of Babylon, in Partial Fulfilment of the Requirements for the Bachelor's degree in Information Security of Information Technology.

By
Sarab kaiser hatam

Supervised by
M.D. Muayad Najm Abdullah

2023-2024

ABSTRACT

wireless networks have security issues that are vulnerable to a variety of attacks. Due to using radio to transport data, attackers can bypass firewalls, sniff sensitive information, intercept packets and send malicious packets. Security auditing and penetration testing is expected to ensure wireless networks security. The contributions of this project are analyzed the vulnerability and types of attacks pertaining to IEEE802.11 WLAN, performed well known attacks in a laboratory environment to conduct penetration tests to confirm whether our wireless network is hackable or not. Aircrack-ng is configured as auditing tool to view wireless attacks, such as WEP/WPA/WPA2 cracking, rouge access points,and attack. Aircrack-ng is designed to detect wireless intrusion with additional features. Penetration testing and auditing will mitigate the risk and threatening to protect WALN.